nextron systems

VALHALLA

VALHALLA

nextron systems

Supercharge Your Detection

Valhalla boosts your detection capabilities with the power of thousands of hand-crafted high-quality YARA rules.

Our team curates more than 11,000 quality tested YARA rules in 5 different categories: APT, Hack Tools, Malware, Web Shells and Exploits. Valhalla's database grows by 1500 YARA rules per year.

With access to Valhalla, you can supercharge your detection by adding most of our highly successful THOR scanners' signatures to your own scan engines.

All rules are performance optimised and quality tested against Terabytes of goodware and other data.

Huge Curated Rule Set

Quality Tested

Rich Meta Data

Valhalla provides rich meta data that adds valuable context to each match, such as a web reference, related threat group campaigns, hashes of samples for which the rule was initially created and a list of public samples on which the rule has matched so far.

Meta Data is Key

Each rule contains information about the required YARA version and modules to run that rule.

The API client allows you to retrieve only those rules that your product supports.

The rule's score and tags indicate its reliability and scope. Both can be used to select the perfect rule set for your application.

Smart API

The Python API allows you download the subscribed categories as text or JSON object. It even has presets for well-known products that support YARA scanning like FireEye's appliances, Tenable, Tanium, CarbonBlack or Symantec MAA. It requires no more than 3 lines of code to retrieve the subscribed YARA rule set.

Flexible API

```
from valhallaAPI.valhalla import ValhallaAPI

v = ValhallaAPI(api_key="Your API Key")
response = v.get_rules_text(product="FireEyeEX")
```

VALHALLA

nextron systems

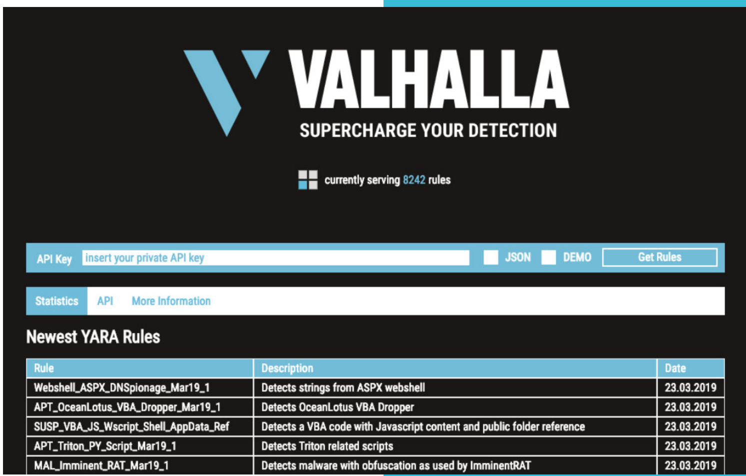
Web Site

The website https://valhalla.nextron-systems.com allows you to immediately retrieve your subscribed rules using nothing but a web browser.

Just insert your API key and click on “Get Rules”.

You can also select the “JSON” checkbox to get them in JSON format or select “DEMO” to test drive this feature with a demo API key, which allows you to retrieve all public YARA rules in the selected format.

The website also contains statistics about the current rule set.



Command Line Client

The comfortable command line client ‘valhalla-cli’ helps to integrate the rule retrieval into your deployment process.

It’s really as simple as it gets.

It can be installed running the following command:

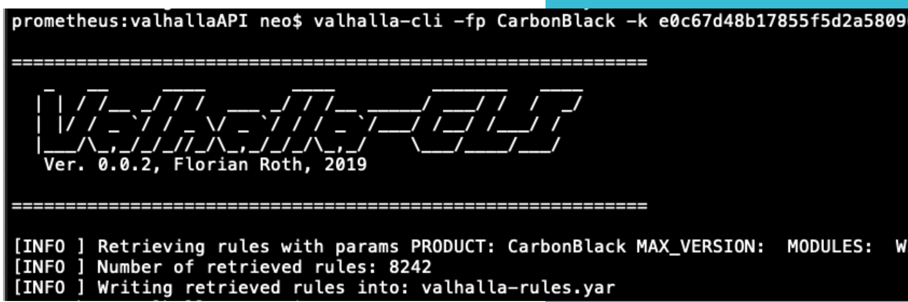
`pip3 install valhallaAPI`

The next command retrieves all subscribed rules:

`valhalla-cli -k APIKEY`

The command line client supports proxy servers and allows you to apply numerous filters, e.g.

- Exclude rules with low scores (e.g. threat hunting rules with scores lower than 75)
- Exclude rules that wouldn’t work on your scan engine (e.g. “Tanium”)
- Retrieve only rules with certain tags (e.g. “CHINA”, “APT”)




```
usage: valhalla-cli [-h] [-k apikey] [-o output-file] [--check] [--debug]
                    [-p proxy-url] [-pu proxy-user] [-pp proxy-pass]
                    [-fp product] [-fv yara-version]
                    [-fm modules [modules ...]] [-ft tags [tags ...]]
                    [-fs score] [-fq query] [--nocrypto]

Valhalla-CLI

optional arguments:
  -h, --help            show this help message and exit
  -k apikey             API KEY
  -o output-file        output file
  --check               Check subscription info and total rule count
  --debug               Debug output

=========================================================================
Proxy:
  -p proxy-url          proxy URL (e.g. https://my.proxy.net:8080)
  -pu proxy-user        proxy user
  -pp proxy-pass        proxy password

=========================================================================
Filter:
  -fp product           filter product (valid products are: FireEyeAX,
                        FireEyeNX, FireEyeEX, CarbonBlack, Tanium, Tenable,
                        SymantecMAA)
  -fv yara-version      get rules that support the given YARA version and
                        lower
  -fm modules [modules ...]
                        set a list of modules that your product supports (e.g.
                        "-fm pe hash") (setting no modules means taht all
                        modules are supported by your product)
  -ft tags [tags ...]   set a list of tags to receive (e.g. "-ft APT MAL")
  -fs score             minimum score of rules to retrieve (e.g. "-fs 75")
  -fq query             get only rules that match a certain keyword in name or
                        description (e.g. "-fq Mimikatz")
  --nocrypto            filter all rules that require YARA to be compiled with
                        crypto support (OpenSSL)
```

VALHALLA

nextron systems

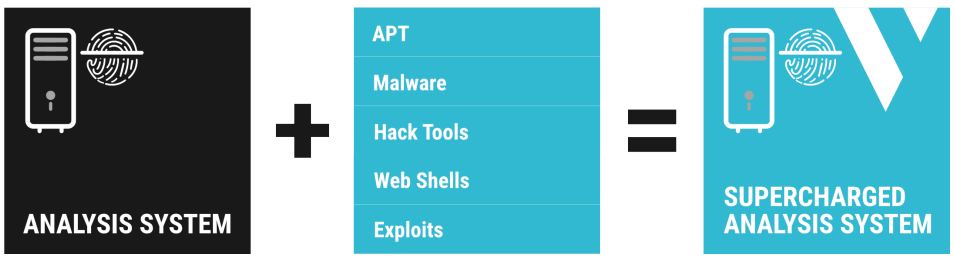
Integration

The web API allows you to retrieve the perfect set that integrates seamlessly with the platform that you use for YARA scanning.

Depending on your use case, we recommend subscriptions for different rule categories.

Curation

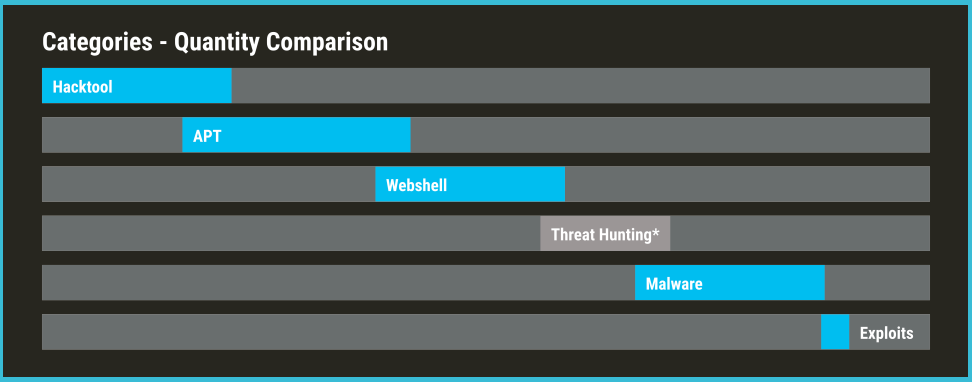
We improve between 300 and 500 old rules per year. These improvements include false positive reductions and the tightening or extension of existing rules.



Supercharge Use Cases

VALHALLA

Valhalla's rule set is divided into 6 categories based on tags that overlap



Special Strength

APT

- High grade rules for malware and tools used by threat groups
- Based on public reports, internal and 3rd party threat intelligence

Web Shells

- More than 1500 web shell rules
- Often very low Antivirus detection ratio (most EDRs miss web shells)

Hack Tools

- Rules to detect a variety of offensive security tools and frameworks
- Rules cover the tool itself, output, helper files and special command line parameters to detect their use in log files

Threat Hunting (only in THOR Scanner)

- Generic rules / heuristic detection methods focus on methods and obfuscation instead of specific threats
- Highly effective in detecting new, yet unknown threats

Growth

The rule set grows by 1000 to 1500 hand-written and quality tested rules per year.

Delivery

You can download the full subscribed set via web browser or use our public API client written in Python to get a customised rule set that fits your scan engine.

Subscription

We offer subscriptions for each of our rule set categories or the whole curated rule set.

Each subscription includes improvements, fixes and updates on the subscribed categories for 12 months.

Trial

We cannot offer a trial of our rule set.

However, the public API allows you to retrieve and test a streamlined demo rule set, which is an equivalent of the public signature-base that is integrated in our free scanners LOKI and SPARK Core.